REMARKS

In response to the Office Action dated November 10, 2003, Applicant respectfully requests reconsideration and withdrawal of the rejections of the claims.

Claim 1 was rejected under 35 U.S.C. §102, on the grounds that it was considered to be anticipated by the Rikuna patent. In addition, all pending claims were rejected under 35 U.S.C. §103, on the basis of the Shona and Turban patents. As discussed in detail hereinafter, none of these three references is directed to the problem addressed by the present invention. Consequently, they do not teach the present invention to a person of ordinary skill in the art, whether considered individually or in combination.

Briefly, the present invention concerns a terminal in a telecommunication network, such as a mobile telephone, that is capable of receiving two different integrated circuit cards. One of these cards is a standard SIM card, which contains information such as the subscriber's identification, security data and communication services. The second card is an application program card containing one or more applications that can be executed within the terminal, such as a banking application. In practice, these two cards might typically be furnished by different entities. For example, the SIM card may be provided to the user by the telecommunications company, whereas the program card might be provided by a bank or merchant.

The present invention is particularly concerned with the security of operations performed within such an environment. In accordance with the invention, before the application contained on the second, program card can be executed, the authenticity of the cards is verified. In an exemplary embodiment disclosed in the application, the SIM card conducts a procedure to authenticate the program card, and vice versa.

It is respectfully submitted that the cited references are not concerned with the same problem as the present invention, and therefore do not teach the solution to such a problem. The Rikuna patent is directed to the fact that, when a user employs an IC card for a transaction, he is often required to enter a personal identification number (PIN). If the user is situated at a location remote from the terminal where the transaction is carried out, e.g. a cash register, the user is inconvenienced by having to go to the location of the terminal. For example, the patent describes a situation where, at a gas station, the user must get out of his car and walk into the station. Alternatively, in a restaurant environment, the waiter must bring a portable terminal to the user.

To overcome this inconvenience, the Rikuna patent discloses an arrangement in which a second IC card is owned by the vendor and presented to the user, into which the user enters his PIN. Thereafter, the vendor inserts both the user's IC card and this second IC card into the transaction terminal. Within the transaction terminal, the PIN stored in the user's IC card is compared with the PIN that was entered on the second IC card, and if they match the transaction is completed. In essence, therefore, the Rikuna patent discloses the use of a second IC card as the medium to transport the user's PIN entry from the location of the user to the location of the transaction terminal, and thereby lessen the inconvenience to the user.

With reference to claim 1, the Office Action states that the Rikuna patent "discloses a processor for pre-controlling the execution of a program contained in a second chip card, inserted in a terminal." It is respectfully submitted, however, that the Rikuna patent does not disclose that the second IC card, i.e. the PIN-entry card, contains a program that is to be executed. Rather, as noted above, the second IC

card merely constitutes a data transport medium, via which the user's PIN is transferred from the location of the user to the location of the transaction terminal. There is no suggestion that this card also contains a *program* that is executed at the terminal.

The Office Action also alleges that the Rikuna patent discloses "a first chip card, containing data and connected to a telecommunication network to which the terminal is linked." Again, however, it is respectfully submitted that the Rikuna patent does not contain such a disclosure. Rather, the patent discloses that the card terminal 12 is associated with the cash register in a restaurant or store. See, for example, column 3, lines 22-23. The patent does not disclose that the terminal is linked to a telecommunication network.

The Office Action goes on to allege that the Rikuna patent discloses the step of "authenticating one of the first and second cards by the other." However, in the system of the Rikuna patent, there is no authentication of one *card* by the other *card*. Rather, the terminal compares the PIN number stored in each of the two IC cards to verify the identity of the *user*. There is no authentication of the cards, per se. Nor is there any authentication performed *by* the card. In each case, they merely function as carriers for the data that is compared within the *terminal*.

For at least the foregoing reasons, therefore, it is respectfully submitted that the Rikuna patent does not anticipate the subject matter of claim 1.

Turning now to the rejections under 35 U.S.C. 103, the Shona patent discloses an arrangement in which an IC card and a host device authenticate one another through the mutual exchange and enciphering of random numbers. As noted in the Office Action, the Shona patent does not disclose the use of a second

chip card, nor a terminal which is linked to a telecommunication network. To this end, therefore, it refers to the Turban patent, which discloses a telecommunication terminal that has the ability to accommodate two chip cards. The patent discloses that the two chip cards can exchange signals and useful data between each other. The Office Action concludes that it would be obvious to combine Shona's mutual authentication system with Turban's plurality of chip cards. It is respectfully submitted, however, that the teachings of these two patents do not lead one to the claimed subject matter, absent hindsight knowledge of the present invention.

The Shona patent is directed to mutual authentication between an IC card and a host device. The host device might be, for example, a terminal that receives the IC card. A logical application of its teachings to the telecommunication terminal of the Turban patent would therefore be the authentication of the terminal and the chip card to one another. This combination, however, does not lead a person of ordinary skill to the present invention.

First, there is no disclosure in the Turban patent that the second chip card is one which contains an application program that is to be executed. The Turban patent discloses very little about the second chip card. Basically, it only discloses that the telecommunications terminal is capable of receiving two chip cards, and that they exchange signals and useful data between one another (column 2, lines 50-53). There is no disclosure that the second card contains an application program to be executed in the terminal. As such, the patent does not disclose any reason why it may be necessary, or useful, to have the chip cards authenticate one another. Only Applicant's application discloses any reason for doing so.

There is no teaching in either of the references that two IC cards in the same terminal should authenticate one another. The Shona patent only pertains to authentication between the IC card and a host device, a procedure which has been carried out in the field of smart cards for many years. The Turban patent discloses that two chip cards can be present in the same terminal, but only vaguely refers to the fact that they might exchange data between them. It does not suggest that there may be security concerns, as between the two cards, and therefore does not teach that it may be appropriate for one to authenticate the other. At best, the combined teachings of the Shona and Turban patents might suggest that each card authenticate itself to the terminal, but there is nothing in these patents to suggest that the cards authenticate themselves to teach other. Only Applicant teaches this concept.

In addition, the references fail to disclose a number of other features recited in the claims. For example, claim 2 recites that the authentication of the second card by the first card includes the step of "applying an identifier of the program which is transmitted from the second card to the first card and a key to an algorithm, contained in the first card, to produce a result." In rejecting claim 2, the Office Action refers to the Shona patent at column 2, lines 63-67. However, this portion of the patent does not disclose transmitting an "identifier of the program" from the second card to the first card (or from the host to the IC card), as recited in the claim. Rather, this portion of the patent discloses that the IC card outputs *a random number*. The Shona patent does not discuss the execution of application programs, and therefore it does not contain any teaching which could be interpreted to suggest utilizing an

identifier of such a program as a data value that is applied to an algorithm to produce an authentication result.

Claim 2 further recites the step of comparing the result "and a certificate which is transmitted by the second card to the first card." Again, there is no disclosure of transmitting a certificate from a second card (or the host) to the first card. The Shona patent only discloses that random numbers are exchanged between the IC card and the host.

Claim 12 recites that the authentication steps are executed in a server of the telecommunication network in response to a request from the first card. The Office Action alleges that the Turban patent discloses this feature, with reference to column 3, lines 37-46. This portion of the patent discloses that the *user* authenticates himself to the network. It does not disclose, nor otherwise suggest, that one of the cards in the telecommunication terminal is authenticated by a remote server, in response to a request from the other card.

Claim 13 recites the steps of reading "characteristics for the execution of the program in the second card, by the first card or the terminal . . . and analysis of the characteristics . . . to reject the second card when said characteristics are incompatible with the first card and/or the terminal." In rejecting this claim, the Office Action refers to the Shona patent at column 2, line 63 to column 3, line 12. However, this portion of the patent merely relates to the procedure by which the IC card and the host exchange random numbers and enciphered data generated from those random numbers. As noted above, the Shona patent does not discuss the execution of a program. Consequently, it cannot be interpreted to disclose the concept of

analyzing characteristics for the execution of a program in order to determine whether to accept or reject a second card.

Claims 14-18 are directed to the various disclosed embodiments for execution of the program stored in the second card. Claim 14 recites that the program is loaded from the second card into the first card, for execution in the first card. Claim 15 recites that the program is executed in the second card, in response to a command from the first card. Claim 18 recites that the program is loaded from the second card into the terminal, for execution in the terminal. As discussed above, neither of the Shona nor Turban patents describes the execution of programs stored on an IC card, particularly a second IC card. The rejection of these claims refers to the Turban patent at column 4, lines 57-64. However, this portion of the patent merely discloses that *data* transmission can be performed between two chip cards. It does not disclose that a program is stored on the second chip card. Furthermore, even if one were to assume that the second chip card contains a program, the Turban patent does not contain any information regarding the manner in which such a program would be executed.

Claims 3, 5 and 9 were rejected under 35 U.S.C. §103 on the basis of the Shona and Turban patents, in further view of the Wasilewski et al patent. Each of these claims recites the step of selecting a key in a table of keys contained in the first card "as a function of the program identifier" that is transmitted from the second card to the first card. In other words, the authentication algorithm key is selected on the basis of the application program to be executed. In rejecting these claims, the Office Action refers to Wasilewski's disclosure of using a random number to generate a key. Even if one were to apply this teaching to the authentication

procedure of the Shona patent, the result would not be the same as the subject matter recited in claims 3, 5 and 9. The claims recite a relationship between the program to be executed and the key that is utilized in the authentication algorithm. Utilizing a random number to generate a key would not result in such a relationship. Rather, the key would be totally independent of any other data being processed.

Claim 6 recites that the authentication process involves the transmission of a predetermined field of a number from the first card to the second card, and comparing the predetermined field to a number in the second card. Claim 7 depends from claim 6, and recites that the predetermined field is the call sign of the telecommunication network that is contained in an identity number of the first card. In rejecting this claim, the Office Action relies upon the Jandrell patent, at column 24, lines 19-27. This portion of the patent pertains to a housekeeping operation that is performed at the beginning of each cycle of data transmission in a communication system. As part of this housekeeping operation, a control center transmits a station identification code, or call sign, to polling stations. It does not, however, disclose nor otherwise suggest the use of a call sign stored in a first IC card as the data which is analyzed to authenticate that first card to a second IC card.

New claims 20-27 also recite these distinguishing features. For instance, claim 20 recites that the authentication of the second card is based upon program information that is transmitted from the second card to the first card. As discussed above, the references do not pertain to the execution of a program stored in a second card, and hence cannot suggest information about such a program as the basis for authenticating the card.

For at least the foregoing reasons, therefore, it is respectfully submitted that the cited references do not anticipate, nor otherwise suggest, the claimed subject matter to a person of ordinary skill in the art. Reconsideration and withdrawal of the rejections are therefore respectfully requested.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: February 10, 2004

By: 

James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620